EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances “EMERALD 1997”

‘203 Claim number	Claim Term	EMERALD 1997 (printed publication)
		handlers. … ● **Valid Response Methods**: Various response functions can be made available to the resolver as it receives intrusion reports from its analysis engines or intrusion summaries from subscribees. These are pre-programmed countermeasure methods that the resolver may invoke as intrusion summaries are received.” p. 358 [SYM_P_0068836] “Implementation of the response policy, including coordinating the dissemination of the analysis results, is the responsibility of the EMERALD resolver. The resolver is an expert system that receives the intrusion and suspicion reports produced by the profiler and signature engines, and based on these reports invokes the various response handlers defined within the resource object … In addition to its external-interface responsibilities, the resolver operates as a fully functional decision engine, capable of invoking real-time countermeasures in response to malicious or anomalous activity reports produced by the analysis engines. Countermeasures are defined in the response-methods field of the resource object. Included with each valid response method are evaluation metrics for determining the circumstances under which the method should be dispatched. These response criteria involve two evaluation metrics: a threshold metric that corresponds to the measure values and scores produced by the profiler engine, and severity metrics correspond to subsets of the associated attack sequences defined within the resource object. The resolver combines the metrics to formulate its monitor's response policy. Aggressive responses may include direct countermeasures such as closing connections or terminating processes. More passive responses may include the dispatching of integrity-checking handlers to verify the operating state of the analysis target.” p. 360-61 [SYM_P_0068838- SYM_P_0068839]
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and	“Monitors also incorporate a versatile application programmers’ interface that enhances their ability to interoperate with the analysis target, and with other third-party intrusion-detection tools.” p. 356 [SYM_P_0068834] “Interoperability is especially critical to EMERALD's decentralized monitoring scheme, and extends within EMERALD's own

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances “EMERALD 1997”

‘203 Claim number	Claim Term	EMERALD 1997 (printed publication)
	integration of third-party tools.	architectural scope as well as to third-party modules. … Third-party modules may also submit and receive analysis results via the resolver's external interfaces. This will allow third-party modules to incorporate the results from EMERALD monitors into their own surveillance efforts, or to contribute their results to the EMERALD analysis hierarchy. Lastly, the monitor's internal API allows third-party analysis engines to be linked directly into the monitor boundary.” p. 357 [SYM_P 0068835]
5	The method of claim 1, wherein the enterprise network is a TCP/IP network.	*“The EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) environment is a distributed scalable tool suite for tracking malicious activity through and across large networks. EMERALD introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response. It combines models from research in distributed high-volume event-correlation methodologies with over a decade of intrusion detection research and engineering experience. The approach is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various abstract layers in a large network. These monitors contribute to a streamlined event-analysis system that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services on the Internet.”* p. 353 [SYM_P_0068831] “The typical target environment of the EMERALD project is a large enterprise network with thousands of users connected in a federation of independent administrative *domains*. Each administrative domain is viewed as a collection of local and network services that provide an interface for requests from individuals internal and external to the domain. Network services include features common to many network operating systems such as mail, HTTP, FTP, remote login, network file systems, finger, Kerberos, and SNMP. Some domains may share trust relationships with other domains (either peer-to-peer or hierarchical). Other domains may operate in complete mistrust of all others, providing outgoing connections only, or perhaps severely restricting incoming connections. Users may be local to a single domain or may possess accounts on multiple domains that allow them to freely establish connections throughout the

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
		enterprise." p. 354 [SYM_P_0068832]
6	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	"Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces). Service monitors may interact with their environment passively (reading activity logs) or actively via probing to supplement normal event gathering." p. 355 [SYM_P_0068833] "Event Generation and Storage: Audit generation and storage has tended to be a centralized activity, and often gathers excessive amounts of information at inappropriate layers of abstraction. Centralized audit mechanisms place a heavy burden on the CPU and I/O throughput, and simply do not scale well with large user populations. In addition, it is difficult to extend centralized audit mechanisms to cover spatially distributed components such as network infrastructure (e.g., routers, filters, DNS, firewalls) or various common network services." p. 354 [SYM_P_0068832]
7	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	"The EMERALD reusable-monitor architecture provides a framework for the organization and coordination of distributed event analysis across multiple administrative domains. EMERALD introduces a service-oriented, layered approach to representing, analyzing, and responding to network misuse. EMERALD's profiling and signature analyses are not performed as monolithic analyses over an entire domain, but rather are deployed sparingly throughout a large enterprise to provide focused protection of key network assets vulnerable to attack. This model leads to greater flexibility whenever the network configuration changes dynamically, and to improved performance, where computational load is distributed efficiently among network resources." p. 363 [SYM_P_0068841] "Domains under EMERALD surveillance are able to detect malicious activity targeted against their network services and infrastructure, and disseminate this information in a coordinated and secure way to other EMERALD monitors (as well as third-party analysis tools) distributed throughout the network. Reports of problems found in one domain can propagate to other monitors throughout the network using the subscription process. EMERALD's subscription-based communication strategy provides mutual

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
		authentication between participants, as well as confidentiality and integrity for all intermonitor message traffic (see Section III-F)." p. 363 [SYM_P_0068841] "Domain-wide analysis forms the second tier of EMERALD's layered network surveillance scheme. A *domain monitor* is responsible for surveillance over all or part of the domain. *Domain monitors* correlate intrusion reports disseminated by individual service monitors, providing a domain-wide perspective of malicious activity (or patterns of activity). In addition to domain surveillance, the domain monitor is responsible for reconfiguring system parameters, interfacing with other monitors beyond the domain, and reporting threats against the domain to administrators. Lastly, EMERALD enables enterprise-wide analysis, providing a global abstraction of the cooperative community of domains. Enterprise-layer monitors correlate activity reports produced across the set of monitored domains. Enterprise-layer monitors focus on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, and coordinated attacks from multiple domains against a single domain. Through this correlation and sharing of analysis results, reports of problems found by one monitor may propagate to other monitors throughout the network." p. 356 [SYM_P_0068834] "Domain monitors may also operate within an enterprise hierarchy, where they disseminate intrusion reports to enterprise monitors for global correlation. Where trust exists between domains, peer-to-peer subscription provides a useful technique for keeping domains sensitized to malicious activity occurring outside their view. Enterprise-layer monitors attempt to model and detect coordinated efforts to infiltrate domain perimeters or prevent interconnectivity between domains. Enterprise surveillance may be used where domains are interconnected under the control of a single organization, such as a large privately owned WAN. Enterprise surveillance is very similar to domain surveillance: the *enterprise monitor* subscribes to various domain monitors, just as the domain monitors subscribed to various local service monitors. The enterprise monitor (or monitors, as it would be important to avoid centralizing any analysis) focuses on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, or coordinated attacks from multiple domains against a single domain." p. 363 [SYM_P_0068841]

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances
"EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
8	The method of claim 7, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	"Domain-wide analysis forms the second tier of EMERALD's layered network surveillance scheme. A *domain monitor* is responsible for surveillance over all or part of the domain. *Domain monitors* correlate intrusion reports disseminated by individual service monitors, providing a domain-wide perspective of malicious activity (or patterns of activity). In addition to domain surveillance, the domain monitor is responsible for reconfiguring system parameters, interfacing with other monitors beyond the domain, and reporting threats against the domain to administrators. Lastly, EMERALD enables enterprise-wide analysis, providing a global abstraction of the cooperative community of domains. Enterprise-layer monitors correlate activity reports produced across the set of monitored domains. Enterprise-layer monitors focus on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, and coordinated attacks from multiple domains against a single domain. Through this correlation and sharing of analysis results, reports of problems found by one monitor may propagate to other monitors throughout the network." p. 356 [SYM_P_0068834] "Domain monitors may also operate within an enterprise hierarchy, where they disseminate intrusion reports to enterprise monitors for global correlation. Where trust exists between domains, peer-to-peer subscription provides a useful technique for keeping domains sensitized to malicious activity occurring outside their view. Enterprise-layer monitors attempt to model and detect coordinated efforts to infiltrate domain perimeters or prevent interconnectivity between domains. Enterprise surveillance may be used where domains are interconnected under the control of a single organization, such as a large privately owned WAN. Enterprise surveillance is very similar to domain surveillance: the *enterprise monitor* subscribes to various domain monitors, just as the domain monitors subscribed to various local service monitors. The enterprise monitor (or monitors, as it would be important to avoid centralizing any analysis) focuses on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, or coordinated attacks from multiple domains against a single domain." p. 363 [SYM_P_0068841]
9	The method of claim 1, wherein deploying the network monitors includes	"Domain-wide analysis forms the second tier of EMERALD's layered network surveillance scheme. A *domain monitor* is responsible for surveillance over all or part of the domain. *Domain monitors* correlate intrusion reports disseminated by individual service monitors, providing a domain-wide perspective of malicious activity (or patterns of activity). In addition to domain surveillance, the

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
	deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	domain monitor is responsible for reconfiguring system parameters, interfacing with other monitors beyond the domain, and reporting threats against the domain to administrators. Lastly, EMERALD enables enterprise-wide analysis, providing a global abstraction of the cooperative community of domains. Enterprise-layer monitors correlate activity reports produced across the set of monitored domains. Enterprise-layer monitors focus on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, and coordinated attacks from multiple domains against a single domain. Through this correlation and sharing of analysis results, reports of problems found by one monitor may propagate to other monitors throughout the network." p. 356 [SYM_P_0068834] "Domain monitors may also operate within an enterprise hierarchy, where they disseminate intrusion reports to enterprise monitors for global correlation. Where trust exists between domains, peer-to-peer subscription provides a useful technique for keeping domains sensitized to malicious activity occurring outside their view. Enterprise-layer monitors attempt to model and detect coordinated efforts to infiltrate domain perimeters or prevent interconnectivity between domains. Enterprise surveillance may be used where domains are interconnected under the control of a single organization, such as a large privately owned WAN. Enterprise surveillance is very similar to domain surveillance: the ***enterprise monitor*** subscribes to various domain monitors, just as the domain monitors subscribed to various local service monitors. The enterprise monitor (or monitors, as it would be important to avoid centralizing any analysis) focuses on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, or coordinated attacks from multiple domains against a single domain." p. 363 [SYM_P_0068841]
10	The method of claim 9, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the	"Domain-wide analysis forms the second tier of EMERALD's layered network surveillance scheme. A *domain monitor* is responsible for surveillance over all or part of the domain. *Domain monitors* correlate intrusion reports disseminated by individual service monitors, providing a domain-wide perspective of malicious activity (or patterns of activity). In addition to domain surveillance, the domain monitor is responsible for reconfiguring system parameters, interfacing with other monitors beyond the domain, and reporting threats against the domain to administrators. Lastly, EMERALD enables enterprise-wide analysis, providing a global abstraction of the cooperative community of domains. Enterprise-layer monitors correlate activity reports produced across the set of monitored domains.

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
	enterprise network.	Enterprise-layer monitors focus on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, and coordinated attacks from multiple domains against a single domain. Through this correlation and sharing of analysis results, reports of problems found by one monitor may propagate to other monitors throughout the network." p. 356 [SYM_P_0068834] "Domain monitors may also operate within an enterprise hierarchy, where they disseminate intrusion reports to enterprise monitors for global correlation. Where trust exists between domains, peer-to-peer subscription provides a useful technique for keeping domains sensitized to malicious activity occurring outside their view. Enterprise-layer monitors attempt to model and detect coordinated efforts to infiltrate domain perimeters or prevent interconnectivity between domains. Enterprise surveillance may be used where domains are interconnected under the control of a single organization, such as a large privately owned WAN. Enterprise surveillance is very similar to domain surveillance: the *enterprise monitor* subscribes to various domain monitors, just as the domain monitors subscribed to various local service monitors. The enterprise monitor (or monitors, as it would be important to avoid centralizing any analysis) focuses on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, or coordinated attacks from multiple domains against a single domain." p. 363 [SYM_P_0068841]
11	The method of claim 9, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	"Where mutual trust among domains exists, domain monitors may establish peer relationships with one another. Peer-to-peer subscription allows domain monitors to share intrusion summaries from events that have occurred in other domains. Domain monitors may use such reports to dynamically sensitize their local service monitors to malicious activity found to be occurring outside the domain's visibility. Domain monitors may also operate within an enterprise hierarchy, where they disseminate intrusion reports to enterprise monitors for global correlation. Where trust exists between domains, peer-to-peer subscription provides a useful technique for keeping domains sensitized to malicious activity occurring outside their view." p. 363 [SYM_P_0068841]
12	An enterprise network	See '203 claim 1

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
	monitoring system comprising:	
	a plurality of network monitors deployed within an enterprise network;	See '203 claim 1
	said plurality of network monitors detecting suspicious network activity	See '203 claim 1
	based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};	See '203 claim 1
	said network monitors generating reports of said suspicious activity; and	See '203 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical	See '203 claim 1

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances “EMERALD 1997”

‘203 Claim number	Claim Term	EMERALD 1997 (printed publication)
	monitors adapted to automatically receive and integrate the reports of suspicious activity.	
13	The system of claim 12, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See ‘203 claim 2
14	The system of claim 12, wherein the integration further comprises invoking countermeasures to a suspected attack.	See ‘203 claim 3
15	The system of claim 12, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See ‘203 claim 4
16	The system of claim 12, wherein the enterprise network is a TCP/IP network.	See ‘203 claim 5

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
17	The system of claim 12, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '203 claim 6
18	The system of claim 12, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7
19	The system of claim 18, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8
20	The system of claim 12, wherein the plurality of	See '203 claim 9

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
	network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	
21	The system of claim 20, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10
22	The system of claim 20, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'212 Claim number	Claim Term	EMERALD 1997 (printed publication)
1	Method for monitoring an enterprise network, said method comprising the steps of:	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1
	based on analysis of network traffic data,	See '203 claim 1
	wherein at least one of the network monitors utilizes a statistical detection method;	"EMERALD's *profiler engine* performs statistical profile-based anomaly detection given a generalized event stream of an analysis target (Section III-C)." p. 356 [SYM_P_0068834] "Requirements for an anomaly-detection system that became IDES were documented in [6]. This research led to the development of the NIDES statistical profile-based anomaly-detection subsystem (NIDES/Stats), which employed a wide range of multivariate statistical measures to profile the behavior of individual users [9]. Analysis is user-based, where a statistical score is assigned to each user's session representing how closely currently observed usage corresponds to the established patterns of usage for that individual. The input source to the NIDES statistical component is an unfiltered and unsorted host audit log, which represents the activity of all users currently operating on the host. In 1995, SRI conducted research under Trusted Information Systems' Safeguard project to extend NIDES/Stats to profile the behavior of individual applications [2]. Statistical measures were customized to measure and differentiate the proper operation of an

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'212 Claim number	Claim Term	EMERALD 1997 (printed publication)
		application from operation that may indicate Trojan horse substitution. Under the Safeguard model, analysis is application-based, where a statistical score is assigned to the operation of applications and represents the degree to which current behavior of the application corresponds to its established patterns of operation. The Safeguard effort demonstrated the ability of statistical profiling tools to clearly differentiate the scope of execution among general-purpose applications. While NIDES/Stats has been reasonably successful profiling users and later applications, it will be extended to the more general subject class typography required by EMERALD. Nonetheless, the underlying mechanisms are well suited to the problem of network anomaly detection, with some adaptation. The required modifications center around extensive reworking of NIDES/Stats to abstract and generalize its definition of measures and profiles, the streamlining of its profile management, and the adaptation of the configuration and reporting mechanisms to EMERALD's highly interoperable and dynamic message system interface. The EMERALD profiler engine achieves total separation between profile management and the mathematical algorithms used to assess the anomaly of events. Profiles are provided to the computational engine as classes defined in the resource object. The mathematical functions for anomaly scoring, profile maintenance, and updating function in a fully general manner, not requiring any underlying knowledge of the data being analyzed beyond what is encoded in the profile class. The event-collection interoperability supports translation of elementary data (the analysis target's event stream) to the profile and measure classes. At that point, analysis for different types of monitored entities is mathematically similar. This approach imparts great flexibility to the analysis in that fading memory constants, update frequency, measure type, and so on are tailored to the entity being monitored. Each profiler engine is dedicated to a specific target event stream at the elementary level. Such localized, target-specific analyses (unlike the monolithic approach employed by NIDES/Stats) provide a more distributed, building-block approach to monitoring, and allow profiling computations to be efficiently dispersed throughout the network. Because the event stream submitted to the profiler engine is specific to the analysis target's activity, profile management is greatly simplified, in that there is no need to support multisubject profile instantiations. In addition, the results of service-layer profiler engines can be propagated to other monitors operating higher in EMERALD's layered analysis scheme, offering domain- or enterprise-wide statistical profiling of anomaly reports. Profiler engines may operate throughout the analysis hierarchy, further correlating and merging service-layer profiles to identify more widespread anomalous activity. The underlying mathematics are the same for each instance, and all required information specific to the entity being monitored (be it a network resource or other EMERALD monitors producing analysis results at lower layers in the analysis

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'212 Claim number	Claim Term	EMERALD 1997 (printed publication)
		hierarchy) is entirely encapsulated in the objects of the profile class." p. 359 [SYM_P_0068837] "The basic analysis unit in this architecture is the EMERALD monitor, which incorporates both signature analysis and statistical profiling. By separating the analysis semantics from the analysis and response logic, EMERALD monitors can be easily integrated throughout EMERALD's layered network surveillance strategy." p. 364 [SYM_P_0068842] 103: A. Valdes and D. Anderson, *Statistical Methods for Computer Usage Anomaly Detection Using NIDES*, Proc. of the Third International Workshop on Rough Sets and Soft Computing, January 1995 ("*Statistical Methods*") [SYM_P_0068937-942].
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1
2	The method of claim 1, wherein at least one of the network monitors utilizes a signature matching detection method.	"The generic EMERALD monitor architecture is illustrated in Figure 1. The architecture is designed to enable the flexible introduction and deletion of analysis engines from the monitor boundary as necessary. In its dual-analysis configuration, an EMERALD monitor instantiation combines signature analysis with statistical profiling to provide complementary forms of analysis over the operation of network services and infrastructure." ... EMERALD's *profiler engine* performs statistical profile-based anomaly detection given a generalized event stream of an analysis

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'212 Claim number	Claim Term	EMERALD 1997 (printed publication)
		target (Section III-C). EMERALD's *signature engine* requires minimal state-management and employs a rule-coding scheme that breaks from traditional expert-system techniques to provide a more focused and distributed signature-analysis model (Section III-D)." p. 356 [SYM_P_0068834] "*D. Scalable Signature Analysis* Signature analysis is a process whereby an event stream is mapped against abstract representations of event sequences that are known to indicate undesirable activity. However, simplistic event binding alone may not necessarily provide enough indication to ensure the accurate detection of the target activity. Signature analyses must also distinguish whether an event sequence being witnessed is actually transitioning the system into the anticipated compromised state. Additionally, determining whether a given event sequence is indicative of an attack may be a function of the preconditions under which the event sequence is performed. To enable this finer granularity of signature recognition, previous efforts have employed various degrees of state detection and management logic (one such example is found in [18]). However, as discussed in Section II, the incorporation of sophisticated rule- and state-management features must be balanced with the need to ensure an acceptable level of performance. In many respects, EMERALD's signature-analysis strategy departs from previous centralized rule-based efforts. EMERALD employs a highly distributed analysis strategy that, with respect to signature analysis, effectively modularizes and distributes the rule-base and inference engine into smaller, more focused signature engines. This has several benefits beyond the performance advantages from evenly distributing the computational load across network resources." p. 359-60 [SYM_P_0068837- SYM_P_0068838]
3	The method of claim 2, wherein the monitor utilizing a signature matching detection method also utilizes a statistical detection method.	See '212 claim 2 and: "In its dual-analysis configuration, an EMERALD monitor instantiation combines signature analysis with statistical profiling to provide complimentary forms of analysis over the operation of network services and infrastructure. … Multiple analysis engines implementing different analysis methods may be employed to analyze a variety of event streams that

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'212 Claim number	Claim Term	EMERALD 1997 (printed publication)
		pertain to the same analysis target." p. 356 [SYM_P_0068834] "The original groundwork for SRI's IDES effort was performed over a decade ago. The first-generation statistics component was used to analyze System Management Facility (SMF) records from an IBM mainframe system [10] in the first half of the 1980s. Requirements for an anomaly-detection system that became IDES were documented in [6]. This research led to the development of the NIDES statistical profile-based anomaly-detection subsystem (NIDES/Stats), which employed a wide range of multivariate statistical measures to profile the behavior of individual users [9]. Analysis is user-based, where a statistical score is assigned to each user's session representing how closely currently observed usage corresponds to the established patterns of usage for that individual. The input source to the NIDES statistical component is an unfiltered and unsorted host audit log, which represents the activity of all users currently operating on the host. ... While NIDES/Stats has been reasonably successful profiling users and later applications, it will be extended to the more general subject class typography required by EMERALD. Nonetheless, the underlying mechanisms are well suited to the problem of network anomaly detection, with some adaptation. The required modifications center around extensive reworking of NIDES/Stats to abstract and generalize its definition of measures and profiles, the streamlining of its profile management, and the adaptation of the configuration and reporting mechanisms to EMERALD's highly interoperable and dynamic message system interface." p. 359 [SYM_P_0068837]
4	The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
5	The method of claim 1, wherein integrating further	See '203 claim 3

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'212 Claim number	Claim Term	EMERALD 1997 (printed publication)
	comprises invoking countermeasures to a suspected attack.	
6	The method of claim 1, wherein the plurality of network monitors includes an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
7	The method of claim 1, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
8	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	"Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces). Service monitors may interact with their environment passively (reading activity logs) or actively via probing to supplement normal event gathering." p. 355 [SYM_P_0068833] "Event Generation and Storage: Audit generation and storage has tended to be a centralized activity, and often gathers excessive amounts of information at inappropriate layers of abstraction. Centralized audit mechanisms place a heavy burden on the CPU and I/O throughput, and simply do not scale well with large user populations. In addition, it is difficult to extend centralized audit mechanisms to cover spatially distributed components such as network infrastructure (e.g., routers, filters, DNS, firewalls) or various common network services." p. 354 [SYM_P_0068832]
9	The method of claim 1, wherein deploying the	See '203 claim 7

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'212 Claim number	Claim Term	EMERALD 1997 (printed publication)
	network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	
10	The method of claim 9, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8
11	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
12	The method of claim 11, wherein receiving and integrating is performed by an	See '203 claim 10

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'212 Claim number	Claim Term	EMERALD 1997 (printed publication)
	enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	
13	The method of claim 11, wherein the plurality of the domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11
14	An enterprise network monitoring system comprising:	See '212 claim 1
	a plurality of network monitors deployed within an enterprise network;	See '212 claim 1
	said plurality of network monitors detecting suspicious network activity	See '212 claim 1
	based on analysis of network traffic data,	See '212 claim 1
	wherein at least one of the network monitors utilizes a statistical detection method;	See '212 claim 1
	said network monitors generating reports of said	See '212 claim 1

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'212 Claim number	Claim Term	EMERALD 1997 (printed publication)
	suspicious activity; and	
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '212 claim 1
15	The system of claim 14, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
16	The system of claim 14, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
17	The system of claim 14, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'212 Claim number	Claim Term	EMERALD 1997 (printed publication)
18	The system of claim 14, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
19	The system of claim 14, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '212 claim 8
20	The system of claim 14, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7
21	The system of claim 20, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8
22	The system of claim 14,	See '203 claim 9

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'212 Claim number	Claim Term	EMERALD 1997 (printed publication)
	wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	
23	The system of claim 22, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10
24	The system of claim 22, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};	See '203 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1
2	The method of claim 1, wherein integrating	See '203 claim 2

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	comprises correlating intrusion reports reflecting underlying commonalities.	
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
5	The method of claim 1, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
6	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '212 claim 8
7	The method of claim 1, wherein at least one of said network monitors utilizes a statistical detection method.	See '212 claim 1
8	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7
9	The method of claim 8, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated	See '203 claim 8

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	network domain.	
10	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
11	The method of claim 10, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10
12	The method of claim 10, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11
13	An enterprise network monitoring system comprising:	See '615 claim 1
	a plurality of network monitors deployed within an enterprise network,	See '615 claim 1
	said plurality of network monitors detecting suspicious network activity	See '615 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network	See '615 claim 1

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances
"EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};	
	said network monitors generating reports of said suspicious activity; and	See '615 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '615 claim 1
14	The system of claim 13, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
15	The system of claim 13, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
16	The system of claim 13, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
17	The system of claim 13, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
18	The system of claim 13, wherein the network	See '212 claim 8

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances
"EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	
19	The system of claim 13, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7
20	The system of claim 19, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8
21	The system of claim 13, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
22	The system of claim 21, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10
23	The system of claim 21, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer	See '203 claim 11

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	relationships with one another.	
34	A computer-automated method of hierarchical even monitoring and analysis within an enterprise network comprising:	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a gateway;	"Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces). Service monitors may interact with their environment passively (reading activity logs) or actively via probing to supplement normal event gathering." p. 355 [SYM_P_0068833] "Event Generation and Storage: Audit generation and storage has tended to be a centralized activity, and often gathers excessive amounts of information at inappropriate layers of abstraction. Centralized audit mechanisms place a heavy burden on the CPU and I/O throughput, and simply do not scale well with large user populations. In addition, it is difficult to extend centralized audit mechanisms to cover spatially distributed components such as network infrastructure (e.g., routers, filters, DNS, firewalls) or various common network services." p. 354 [SYM_P_0068832]
	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data;	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1
35	The method of claim 34, wherein said integrating comprises correlating intrusion	See '203 claim 2

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	reports reflecting underlying commonalities.	
36	The method of claim 34, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
37	The method of claim 34, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
38	The method of claim 34, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1
39	The method of claim 34, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7
40	The method of claim 39, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8
41	The method of claim 34, wherein said	See '203 claim 9

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	
42	The method of claim 41, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10
43	The method of claim 41, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11
44	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a router;	"Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces). Service monitors may interact with their environment passively (reading activity logs) or actively via probing to supplement normal event gathering." p. 355 [SYM_P_0068833] "Event Generation and Storage: Audit generation and storage has tended to be a centralized activity, and often gathers excessive amounts of information at inappropriate layers of abstraction. Centralized audit mechanisms place a heavy burden on the CPU and I/O throughput, and simply do not scale well with large user populations. In addition, it is difficult to extend centralized audit mechanisms to cover spatially distributed components such as

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
		network infrastructure (e.g., routers, filters, DNS, firewalls) or various common network services." p. 354 [SYM_P_0068832]
	detecting, by the network monitors, suspicious network activity based on analysis of the network traffic data;	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1
45	The method of claim 44, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
46	The method of claim 44, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
47	The method of claim 44, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
48	The method of claim 44, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume,	See '615 claim 1

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	network connection requests, network connection denials, error codes included in a network packet}.	
49	The method of claim 44, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7
50	The method of claim 49, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8
51	The method of claim 44, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
52	The method of claim 51, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10
53	The method of claim 51, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships	See '203 claim 11

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	with one another.	
64	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a firewall;	"Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces). Service monitors may interact with their environment passively (reading activity logs) or actively via probing to supplement normal event gathering." p. 355 [SYM_P_0068833] "Event Generation and Storage: Audit generation and storage has tended to be a centralized activity, and often gathers excessive amounts of information at inappropriate layers of abstraction. Centralized audit mechanisms place a heavy burden on the CPU and I/O throughput, and simply do not scale well with large user populations. In addition, it is difficult to extend centralized audit mechanisms to cover spatially distributed components such as network infrastructure (e.g., routers, filters, DNS, firewalls) or various common network services." p. 354 [SYM_P_0068832]
	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data;	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1
65	The method of claim 64, wherein said integrating comprises correlating intrusion	See '203 claim 2

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	reports reflecting underlying commonalities.	
66	The method of claim 64, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
67	The method of claim 64, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
68	The method of claim 64, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1
69	The method of claim 64, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7
70	The method of claim 69, wherein said receiving and integrating is preformed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8
71	The method of claim 64, wherein said	See '203 claim 9

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	
72	The method of claim 71, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10
73	The method of claim 71, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11
84	An enterprise network monitoring system comprising:	See '615 claim 1
	a plurality of network monitors deployed within an enterprise network, wherein at least one of the network monitors is deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers, firewalls}, said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data;	"Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces). Service monitors may interact with their environment passively (reading activity logs) or actively via probing to supplement normal event gathering." p. 355 [SYM_P_0068833] "Event Generation and Storage: Audit generation and storage has tended to be a centralized activity, and often gathers excessive amounts of information at inappropriate layers of abstraction. Centralized audit mechanisms place a heavy burden on the CPU and I/O throughput, and simply do not scale well with large user populations. In addition, it is difficult to extend centralized audit mechanisms to cover spatially distributed components such as network infrastructure (e.g., routers, filters, DNS, firewalls) or various common network services."

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
		p. 354 [SYM_P_0068832]
	said network monitors generating reports of said suspicious activity; and	See '615 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '615 claim 1
85	The system of claim 84, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
86	The system of claim 84, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
87	The system of claim 84, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
88	The system of claim 84, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a	See '615 claim 1

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
	network packet}.	
89	The system of claim 84, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7
90	The system of claim 89, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8
91	The system of claim 84, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
92	The system of claim 91, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'615 Claim number	Claim Term	EMERALD 1997 (printed publication)
93	The system of claim 91, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11